

KINGSBOROUGH COMMUNITY COLLEGE
The City University of New York

CURRICULUM TRANSMITTAL COVER PAGE

Department: Department of Mathematics & Computer Science Date: 6/01/2026

Title Of Course/Degree/Concentration/Certificate: Cybersecurity (CIS 4600)

Change(s) Initiated: (Please check)

- | | |
|--|---|
| ☐ Closing of Degree | ☐ Change in Degree or Certificate |
| ☐ Closing of Certificate | ☐ Change in Degree: Adding Concentration |
| ☐ New Certificate Proposal | ☐ Change in Degree: Deleting Concentration |
| ☐ New Degree Proposal | ☐ Change in Prerequisite, Corequisite, and/or Pre/Co-requisite |
| ☒ New Course | ☐ Change in Course Designation |
| ☐ New 82 Course (Pilot Course) | ☐ Change in Course Description |
| ☐ Deletion of Course(s) | ☐ Change in Course Title, Number, Credits and/or Hours |
| | ☐ Change in Academic Policy |
| | ☐ Pathways Submission: |
| | ☐ Life and Physical Science |
| | ☐ Math and Quantitative Reasoning |
| | ☐ A. World Cultures and Global Issues |
| | ☐ B. U.S. Experience in its Diversity |
| | ☐ C. Creative Expression |
| | ☐ D. Individual and Society |
| | ☐ E. Scientific World |
| ☐ Change in Program Learning Outcomes | |
| ☐ Other (please describe): _____ | |

PLEASE ATTACH MATERIAL TO ILLUSTRATE AND EXPLAIN ALL CHANGES

DEPARTMENTAL ACTION

Action by Department and/or Departmental Committee, if required:

Date Approved: 07/17/2026 Signature, Committee Chairperson: 

If submitted Curriculum Action affects another Department, signature of the affected Department(s) is required:

Date Approved: _____ Signature, Department Chairperson: _____

Date Approved: _____ Signature, Department Chairperson: _____

I have reviewed the attached material/proposal

Signature, Department Chairperson: 



TO: Fall 2026 Curriculum Committee

FROM: Prof. Yarmish, Chair, Department of Mathematics & Computer Science

DATE: 6/1/2026

RE: New Course: Cybersecurity (CIS 4600)

The Department of Mathematics & Computer Science is proposing a new course as follows:

ADD:

Cybersecurity (CIS 4600)

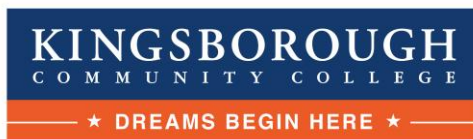
Rationale for Change:

This course will fill a growing need in the department's offerings by providing students with a comprehensive introduction to cybersecurity principles, practices, and current security challenges affecting individuals, organizations, and society.

Current Computer Science and CIS offerings primarily emphasize programming and technical concepts, while this course will focus specifically on the protection of digital systems, networks, and information assets. Students will examine topics such as cybersecurity threats, risk management, data protection, ethical and legal considerations, and security best practices, while gaining practical exposure to foundational cybersecurity tools and techniques.

The course will also address the increasing importance of cybersecurity awareness in today's technology-driven environment and prepare students to better understand the technical, ethical, and societal implications of information security in both personal and professional contexts.

Upon successful completion of the course, students will also be prepared for the CompTIA Cybersecurity Analyst (CySA+) (V3) certification exam.



New Course Proposal Form

1. Complete the requested course information in the table below. Indicate “**NONE**” where applicable.

*For Assignment of New Course Number, contact **Academic Scheduling**.

Department:	Mathematics and Computer Science
Course Designation/Prefix:	CIS
*Course Number:	4600
Course Title:	Cybersecurity
Course Description: (Description should include language similar to Course Learning Outcomes)	This course provides students with a comprehensive introduction to the principles, practices, and technologies used to protect information systems, networks, and organizational data from cyber threats. Students will examine the evolving cybersecurity landscape, including common attack methods, system vulnerabilities, and risk management strategies. Through hands-on activities learners will develop foundational skills in securing computer systems, implementing security controls, conducting vulnerability assessments, and analyzing network and system security architectures. The course emphasizes the application of security best practices, including access control, encryption, firewalls, intrusion detection and prevention systems, secure system configuration, and user awareness strategies. Students will gain practical experience using industry-standard cybersecurity tools and methodologies to assess and strengthen security posture. By the end of the course, students will be prepared to identify, evaluate, and mitigate cybersecurity risks while supporting the confidentiality, integrity, and availability of information assets within diverse organizational environments. The course also prepares students for the CompTIA Cybersecurity Analyst (CySA+) (V3) certification.
Prerequisite(s):	CIS 15
Corequisite(s):	None
Pre-/Co-requisite(s):	None

Indicate if: - Open ONLY to Select Student Population(s) OR - Specific Student Population(s) are RESTRICTED from enrollment in the course Specify Population	
Frequency course is to be offered (Select All that Apply)	X Fall ☐ Winter X Spring ☐ Summer
Suggested Class Limit:	25
Indicate if a special space, such as a lab, and/or special equipment will be required:	Computer Lab with all standard college lab software at each station and Internet/Web accessible on all.
Faculty Information:	
Are there currently faculty within the Department available to teach this course?	X Yes* ☐ No*
Does this course require the faculty member to have a specific credential?	☐ Yes* X No
*If yes, please provide a Staffing Plan (see #13)	
Does this course provide an imbedded Microcredential or Industry Certification?	X Yes ☐ No
If yes, please include relevant information	CompTIA Cybersecurity Analyst (CySA+) (V3) certification.

2. Credits and Hours based on MSCHE Guidelines for *College Credits Assigned for Instructional Hours* -*Hours are based on hours per week in a typical 12-week semester (Please check **ONE** box based on credits):

1-credit:	☐ 1 hour lecture ☐ 2 hours lab/field/gym
2-credits:	☐ 2 hours lecture ☐ 1 hour lecture, 2 hours lab/field ☐ 4 hours lab/field
3-credits:	☐ 3 hours lecture X 2 hours lecture, 2 hours lab/field ☐ 1 hour lecture, 4 hours lab/field ☐ 6 hours lab/field
4-credits:	☐ 4 hours lecture ☐ 3 hours lecture, 2 hours lab/field ☐ 2 hours lecture, 4 hours lab/field ☐ 1 hour lecture, 6 hours lab/field ☐ 8 hours lab/field
More than 4-credits:	☐ Number of credits: ____ (explain mix lecture/lab below)

Explanation: _____ Lecture _____ Lab

3. **Where** does this course fit? Select from the following:

☒ Degree Program(s)/Certificate(s)*	List Degree Program(s)/Certificate(s): Computer Information Systems A.A.S. Major
☐ General Education/Pathways	Select ONE of the following: ☐ Life and Physical Science (LPS) ☐ Math and Quantitative Reasoning (MQR) ☐ World Cultures and Global Issues (Group A) ☐ U.S. Experience in its Diversity (Group B) ☐ Creative Expression (Group C) ☐ Individual and Society (Group D) ☐ Scientific World (Group E)
☐ 82XX Pilot/Experimental Course	If proposed as a “real” course, where will this course fit? Select from the following: List Degree Program(s)/Certificate(s): Computer Information Systems A.A.S. Major Select ONE of the following: ☐ Life and Physical Science (LPS) ☐ Math and Quantitative Reasoning (MQR) ☐ World Cultures and Global Issues (Group A) ☐ U.S. Experience in its Diversity (Group B) ☐ Creative Expression (Group C) ☐ Individual and Society (Group D) ☐ Scientific World (Group E)

***If Degree Program/Certificate is Selected:**

- Include an updated **Curricular** Map (Program Learning Outcomes) for each Degree Program/Certificate listed above.
- Include an updated Degree Map (semester-by-semester course sequence) for each Degree Program/Certificate listed above. For Degree Map template, contact Amanda Kalin, ext. 4611, Amanda.Kalin@kbcc.cuny.edu

The Following NYSED Guidelines must be adhered to for **ALL** Degree Programs:

45 credits of Liberal Arts (General Education) course work for an Associate of Arts Degree (AA)
30 credits of Liberal Arts (General Education) course work for an Associate of Science Degree (AS)
20 credits of Liberal Arts (General Education) course work for an Applied Associate of Science (AAS)

Additional Separate Submissions Required:

1. Curriculum Transmittal Cover Page indicating a “Change in Degree or Certificate”
2. Memo with rationale for inclusion of the course within the curriculum
3. “Current” Degree with all proposed deletions (strikeouts) and additions (bolded) clearly indicated
4. “Proposed” Degree, which displays the degree as it will appear in the *College Catalog*
 - a. For a copy of the most up-to-date Degree/Certificate requirements contact Amanda Kalin, ext. 4611, Amanda.Kalin@kbcc.cuny.edu

If General Education/Pathways is Selected:

- [Please refer to NYSED Guidelines for courses that are considered Liberal Arts \(General Education\).](#)
- Pilot/Experimental/82XX courses CANNOT be submitted for Pathways until they are submitted as a “real” course.

Additional Separate Submissions Required:

1. Curriculum Transmittal Cover Page indicating BOTH “New Course” and “Pathways”
 2. CUNY Common Core Pathways Submission Form
4. **List the Course Learning Outcomes:** – Course Learning Outcomes are measureable/demonstrable, containing “**action verbs**” (Blooms Taxonomy). If proposed to PATHWAYS, the Course Learning Outcomes should *significantly* align with the Pathways Learning Outcomes (refer to the Pathways Common Core Submission Form for Pathways Learning Outcomes). If proposed for a Degree program, the course should align with the Program Learning Outcomes (PLOs). **REMINDER** – Course Learning Outcomes are consistent for **ALL sections** of the same course and **MUST** be included on the syllabus.

Course Learning Outcomes
1. Identify and assess cybersecurity threats, vulnerabilities, and risks affecting computer systems, networks, and organizational data.
2. Apply security principles and best practices to protect information systems from cyber attacks and unauthorized access.
3. Analyze network and system security architectures and evaluate their effectiveness in mitigating security threats.
4. Implement basic cybersecurity controls, including firewalls, access controls, encryption, and intrusion detection/prevention mechanisms.
5. Conduct security assessments and vulnerability analyses using industry-standard tools and methodologies.
6. Demonstrate proficiency in secure computing practices, including secure configuration, system hardening, and user awareness strategies.

5. **Assessment of Course Learning Outcomes:** The Course Learning Outcomes are measurable/demonstrable through the below listed sample assignments/activities. Include percentage breakdown for grading.

REMINDER - Assessment of Course Learning Outcomes are based on a **Common Syllabus** – to allow for **any** qualified instructor to teach the course.

Course Learning Outcome	Percentage of Grade	Measurement of Learning Outcome (Artifact/Assignment/Activity)
1. Identify and assess cybersecurity threats, vulnerabilities, and risks affecting computer systems, networks, and organizational data.	20%	Course Exams (Midterm and Final) Laboratory assignments
2. Apply security principles and best practices to protect information systems from cyber attacks and unauthorized access.	20%	Laboratory assignments
3. Analyze network and system security architectures and evaluate their effectiveness in mitigating security threats.	20%	Course Exams (Midterm and Final) Laboratory assignments
4. Implement basic cybersecurity controls, including firewalls, access controls, encryption, and intrusion detection/prevention mechanisms.	10%	Laboratory assignments
5. Conduct security assessments and vulnerability analyses using industry-standard tools and methodologies.	10%	Laboratory assignments
6. Demonstrate proficiency in secure computing practices, including secure configuration, system hardening, and user awareness strategies.	20%	Course Exams (Midterm and Final) Laboratory assignments

The breakdown is:

35% midterm, 35% final, 30% laboratory assignments

6. **Who** is expected to enroll in this course? Please provide details for the student population(s), degree program(s)/certificate(s), and applicable concentration(s), this course is expected to address.

Students in the Computer Information Systems A.A.S. degree
--

7. Explain **why** this course is a necessary addition to the curriculum. **REMINDER** – Explain the course’s role within the selected Pathways Group or Degree program – How does this course meet the Program Learning Outcomes (PLOs)? Was the course a recommendation from a recent Academic Program Review (APR), Advisory Board, Accrediting Body, etc.? How might this course help students upon transfer to a baccalaureate program or transition into a career/workforce after KCC?

A course in **Cybersecurity** is important for a **Computer Information Systems (CIS)** major because modern organizations depend on secure information systems to protect their operations, data, customers, and reputation. CIS professionals are often responsible for designing, managing, and supporting business technology systems, making security knowledge essential rather than optional.

1. Protecting Organizational Data

Organizations store large amounts of sensitive information, including customer records, financial data, employee information, and intellectual property. A cybersecurity course teaches CIS students how to identify vulnerabilities, implement safeguards, and reduce the risk of data breaches and cyberattacks. Cybersecurity education emphasizes protecting information assets and developing effective defenses against threats.

2. Understanding Modern Business Risks

Cyberattacks can result in financial losses, operational disruptions, legal liabilities, and reputational damage. CIS professionals must understand common threats such as phishing, malware, ransomware, insider threats, and network attacks. Courses in cybersecurity provide the knowledge needed to evaluate risks and recommend appropriate security controls.

3. Integrating Security into Information Systems

Information systems professionals design and manage databases, networks, web applications, and enterprise systems. Security must be incorporated into every stage of system development and administration. A cybersecurity course teaches students how to build secure systems rather than adding security after deployment.

4. Meeting Industry and Regulatory Requirements

Many industries must comply with regulations and standards related to information security and privacy. CIS graduates who understand security principles can help organizations meet compliance requirements and avoid penalties resulting from inadequate security practices. Cybersecurity education includes policies and security management concepts that support organizational compliance efforts.

8. **Transfer** – Provide a general explanation of the transferability of this course. Address all of the following in your explanation:
- Will this course meet a specific **degree requirement** in the equivalent baccalaureate program? Include the institution, degree program, and course equivalency.
 - Will this course serve as the equivalent of a freshman/sophomore course (100/200 level)?
 - Do we currently have an Articulation Agreement established (see current [Articulation Agreements](#)) with the transfer institution for the equivalent degree program? If you have a tentative Articulation Agreement/Communication with Chair at the transfer institution, please include.

This course may be equivalent to similar courses at four-year institutions.

City tech

CST 3610 - Network Security Fundamentals (3 cr)

John jay

CSCI 411 Computer Security and Forensics (3 cr)

Baruch

CIS 3550 – Cybersecurity (3 Cr)

BMCC

CIS 455 Network Security (3 cr)

QCC

ET-725 Computer Network Security (3 cr)

LaGuardia

MAC237: Computer Security (3 Cr)

9. Will adding the course potentially **conflict** with other courses – in content or subject matter – offered in either your Department or in *another* Department? If it will, please explain **how** and indicate **why** the course is still necessary.

No

10. Proposed textbook(s) and/or other required instructional material(s), including open educational resources (OER)– Please include any supplemental/recommended materials/texts to allow for **any** qualified instructor to teach the course:

CompTIA Cyber Defense Pro course (courseware)

11. **Attach a Common Syllabus** that includes the Topical Course Outline for the 12-week semester. This should be **specific** and **explicit** regarding the topics covered and should contain the detailed sample assignments/activities being used to measure the Course Learning Outcomes. **REMINDER** – be mindful to focus on the Course Learning Outcomes, Course Content, and Assessment.

12. Selected Bibliography and Source materials:

Cybersecurity Essentials, Charles J. Brooks, Christopher Grow, Philip Craig Jr., Donald Short, Wiley, ISBN: 9781119362456

Network Security Essentials: Applications and Standards (6th Ed.), William Stallings, Pearson, ISBN: 9780137561650

Cryptography and Network Security: Principles and Practice (8th Ed.), William Stallings, Pearson, ISBN: 9780135764213

Computer Security: Principles and Practice (4th Ed.), William Stallings, Lawrie Brown, Pearson, ISBN: 9780134794105

Principles of Information Security (7th Ed.), Michael E. Whitman, Herbert J. Mattord, Cengage Learning ISBN: 9780357506431

Introduction to Cybersecurity: Foundations and Practice, Neal Wagner, CRC Press, ISBN: 9781482236750

Cybersecurity: Attack and Defense Strategies (3rd Ed.), Yuri Diogenes, Erdal Ozkaya, Packt Publishing ISBN: 9781835083307

Security+ Guide to Network Security Fundamentals (7th Ed.), Mark Ciampa, Cengage Learning ISBN: 9780357424377

Practical Malware Analysis, Michael Sikorski, Andrew Honig, No Starch Press, ISBN: 9781593272906

Digital Forensics and Incident Response (3rd Ed.), Jason T. Luttgens, Matthew Pepe, Kevin Mandia, McGraw-Hill, ISBN: 9781264268467

13. **Staffing Plan** – please provide a staffing plan if there are currently **no faculty** within the Department available to teach this course or who do not have the required credential to teach this course.

--

Topical Outline

Week	Session (L=Lab)	Topic	Course* Learning Outcomes	Lecture Hours	Lab Hours
1	1	2.1.1 Regulations and Standards 2.2.1 Risk Management Principles 2.2.2 Applying the Appropriate Risk Strategies 2.2.3 Threat Modeling 2.3.1 Security Control Categories and Types 2.4.2 Set Up Security Appliance Access 2.4.3 Set Up a Captive Portal 2.4.4 Discover Vulnerable Bluetooth Devices 2.4.5 Securing Mobile Devices	1	3	1
	L2	L 2.3.4 Implement Physical Security Countermeasures L 2.4.6 Configure a Captive Portal L 2.4.7 Discover Bluetooth Devices L 2.4.8 Secure a Mobile Device L 2.4.9 Configure a Security Appliance L 2.4.10 Configure Security Appliance Access	2		

	3	2.5.2 Configuration Management 2.5.3 Configure Password Policies 2.5.4 Manage Certificates 2.6.1 Attack Frameworks	3, 4		
	4	2.6.3 MITRE ATT&CK Framework 3.1.1 Threat Actor Types 3.2.2 Reconnaissance with TheHarvester 3.2.3 Reconnaissance with Nmap 3.2.4 Threat Intelligence Types 3.3.1 Threat Hunting Overview 3.3.3 Analyzing Indicators of Compromise (IoC) 3.3.4 Indicators of Compromise (IoC) Facts 3.3.5 Threat Research	5		
2	5	3.3.6 Threat Research Facts 3.4.1 Honeypots 3.4.3 Evade Honeypots 3.4.5 Anti-Malware Software 3.4.7 Detect Malicious Network Traffic with a Honeypot 3.4.8 Scan for Open Ports with Netstat 3.4.9 Track Port Usage with TCPView 4.1.1 View Windows Services 4.1.2 View Linux Services 4.1.4 Scanning and Terminating Processes	3	2	2
	L6	L 2.5.5 Analyze Passwords using Rainbow Tables L 2.5.6 Configure Account Password Policies L 2.5.7 Manage Certificates L 3.4.10 Create a Honeypot with Pentbox	4		
	L7	L 4.1.5 Manage Linux Services L4.1.6 Enable and Disable Linux Services L4.1.7 Disable Windows Services L4.1.8 View Process Information	6		
	8	4.2.1 Virtualization Management Overview 4.2.3 Cloud Computing 4.2.6 Network Architectures 4.3.1 Identity and Access Management 4.3.2 Identity and Access Management Facts 4.3.3 Federation	1		
3	9	4.3.5 Service-Oriented Architecture 4.4.1 Data Loss Prevention (DLP) 4.4.3 Data Monitoring Methods 4.5.1 Log Review Overview 4.5.3 Configure Centralized Logging with Cisco Devices 4.5.4 Use pfSense to Log Events 4.5.5 Evaluate Event Logs in pfSense 4.5.6 Configure Collector-Initiated Subscriptions	3,4	3	1

		4.5.7 Configure Source-Initiated Subscriptions 4.5.8 Log Events with Event Viewer			
	L10	L 4.5.9 Log Events with pfSense L 4.5.10 Evaluate Event Logs in pfSense L 4.5.11 Evaluate Windows Log Files	1		
	11	5.1.1 Reconnaissance Processes 5.1.2 Reconnaissance Tools Facts 5.1.3 Perform a Scan with Nmap 5.1.4 Perform a Scan with Nmap Scripts 5.1.6 NMAP Fingerprint Facts 5.1.7 Scan for IoT with Nmap 5.1.8 Conduct Vulnerability Scans 5.1.9 Disable DNS Zone Transfers	1,3,5		
	12	5.1.11 Extract Web Server Information 5.1.13 Detect Promiscuous Mode 5.1.14 Perform a SYN Flood 5.1.16 Disable IIS Banner Broadcasting 5.2.1 Scanning Overview 5.2.4 Scanning Considerations 5.2.7 Configure a Perimeter Firewall 5.2.8 Avoid Firewall Detection 5.2.9 Bypass Windows Firewall with Metasploit	1,3,5		
4	L13	L 5.1.5 Perform Reconnaissance with Nmap L 5.1.10 Perform an Internal Scan with Nmap L 5.1.12 Extract Web Server Information with Nmap L 5.1.15 Analyze a SYN Flood Attack L 5.1.17 Hide the IIS Banner Broadcast	3,4,5	1	3
	L14	L 5.2.10 Perform an External Scan Using Zenmap L 5.2.11 Detect Open Ports with Nmap L 5.2.12 View Open Ports with netstat L 5.2.13 Bypass Windows Firewall with Nmap L 5.2.14 Scan for Vulnerabilities on IoT L 5.2.15 Troubleshoot Connectivity with ping/hping3	1,5		
	15	5.3.1 Enumeration 5.3.2 Enumerate Operating Systems 5.3.5 Enumerate Windows 5.3.6 Enumerate a Linux System 5.3.7 Enumerate with NetBIOS Enumerator 5.3.8 Enumerate with SoftPerfect 5.3.9 Enumerate with Metasploit	1,6		
	L16	L 5.3.10 Perform Enumeration with Nmap L 5.3.11 Perform Enumeration with Metasploit L 5.3.12 Perform Enumeration of MSSQL with Metasploit	2,6		
5	17	Midterm		3	1

	18	5.4.1 Vulnerability Assessment Tools 5.4.2 Vulnerability Assessment Tool Facts 5.4.6 Vulnerability Scan Analysis 5.4.7 Vulnerability Scan Analysis Facts 5.4.7 Vulnerability Scan Analysis Facts 5.4.8 Configure a Nessus Scan 5.4.9 Analyze Scan Results from a Nessus Report 5.4.10 Inspect HTTP Requests with Tamper Data 5.4.11 Navigate the DVWA Website 5.4.14 Test a Web Application with Burp Suite	1,3,5		
	L19	L 5.4.12 Scan for Vulnerabilities on a Windows Workstation L 5.4.13 Scan for Vulnerabilities on a Linux Server L 5.4.15 Test the Security of a Web Application 1 L 5.4.16 Test the Security of a Web Application 2	1,5,6		
	20	5.5.1 Vulnerability Scoring Systems 5.6.1 Vulnerability Management Life Cycle 5.6.3 Vulnerability Reporting Overview 5.6.7 Action Plans 5.6.11 Inhibitors to Vulnerability Remediation	1,2		
6	21	6.1.1 Security Monitoring 6.1.3 Segmentation 6.1.5 Intrusion Detection System (IDS) 6.1.7 Evade IDS 6.1.9 Intrusion Detection and Prevention with Snort 6.1.10 Intrusion Detection and Prevention with Suricata 6.2.1 Wireless Hacking 6.2.3 Detect a Rogue Device	3,5	2	2
	L22	L 6.1.11 Prevent Zone Transfer L 6.1.12 Implement Intrusion Prevention with pfSense L 6.1.13 Configure a Perimeter Firewall L 6.1.14 Perform a Decoy Scan	4,6		
	L23	L 6.2.5 Scan for Open Ports from a Remote Computer L 6.2.6 Discover a Hidden Network L 6.2.7 Discover a Rogue DHCP Server L 6.2.8 Locate a Rogue Wireless Access Point	1,3		
	24	6.3.1 Web Server Attacks 6.3.3 Scan a Website with Acunetix 6.3.5 Web Application Hacking 6.3.7 Web Application Countermeasures 6.3.9 Set Up a Web Session Hijack 6.3.10 Exploit Cross-Site Scripting Vulnerabilities 6.4.1 SQL Injection 6.4.3 SQL Injection Attack Types	1, 3, 4,5		
7	L25	L 6.3.4 Evaluate Webserver Security L 6.3.11 Hijack a Web Session	1,5,6	2	2

	26	6.4.5 Exploit SQL on a Web Page 6.4.6 Find SQL Injection Flaws with sqlmap 6.4.7 Hidden Field Manipulation Attacks 6.4.8 Explore SQL Injection Flaws 6.4.9 Detect SQL Injection Flaws with Burp Suite	1,4		
	L27	L 6.4.8 Explore SQL Injection Flaws L 6.4.9 Detect SQL Injection Flaws with Burp Suite	1,4		
	28	6.5.1 Sniffing 6.5.3 Sniff Network Traffic with Wireshark 6.5.4 Sniff Network Traffic with TShark 6.5.5 Capture Traffic with TCPDump 6.5.6 Use SMAC to Spoof MAC Addresses 6.5.7 Poison ARP 6.5.8 Poison DNS	3,6		
8	L29	L 6.5.9 Analyze ARP Poisoning with Wireshark L 6.5.10 Analyze DNS Spoofing L 6.5.11 Filter and Analyze Traffic with Wireshark	1	1	3
	30	6.6.1 Identity and Access Management Threats Overview 6.6.3 Client-Side and Network Attacks 6.6.5 Perform an On-Path DHCP Attack 6.7.1 Cloud Security 6.7.3 Use ScoutSuite to Analyze a Cloud Infrastructure 6.7.5 Data Exfiltration 6.7.7 Google Hacking for Office Documents 6.8.1 Email Analysis Overview	1,3		
	L31	L 6.6.6 Analyze a DHCP Spoofing On-Path Attack L 6.6.7 Analyze HTTP POST Packets with Wireshark	3		
	L32	L 6.8.4 Analyze Email Traffic for Spoofed Addresses L 6.8.5 Analyze Email Traffic for Sensitive Data	3		
9	33	6.9.1 DoS Attack Types 6.9.3 DoS Countermeasures 6.9.5 DDoS Attack Types 6.9.7 Signs of a DDoS Attack 6.9.9 Launch a DoS and DDoS Attack 6.10.1 Controller Systems 7.1.1 Device Security Overview 7.1.5 Verify MD5 Hash Integrity 7.1.6 Create a Forensic Drive Image with FTK 7.1.7 Create a Forensic Drive Image with Guymager	1,2,4,6	2	2
	L34	L 6.9.10 Analyze ICMP Traffic in Wireshark L 6.9.11 Analyze a DoS Attack L 6.9.12 Analyze a DDoS Attack	3		
	35	7.1.8 Create a Forensic Drive Image with DC3DD 7.1.9 Examine a Forensic Drive Image with Autopsy	2,4		

		7.1.10 Change File Permissions with icacs 7.1.11 Encrypt Data 7.1.12 Encrypt a Hard Disk 7.1.13 Wipe Disk Space 7.1.14 Recover Deleted Files with Recuva 7.2.1 Privilege Escalation in Windows			
	L36	L 7.1.4 Create a Remote Access Policy L 7.1.15 Encrypt a Hard Drive L 7.1.16 Compare an MD5 Hash L 7.1.17 Examine a Forensic Drive Image	2,4,6		
10	37	7.2.7 Use Bootable Media to Modify User Accounts 7.2.8 Crack the SAM Database 7.2.9 Change a Windows Password 7.2.10 Configure User Account Control 7.2.11 Use Fail2Ban 7.2.12 Escalate Privileges with Curl 7.2.13 Explore Privilege Creep 7.3.1 Malware Overview 7.3.2 Use Windows Defender Application Control	2,4,5	2	2
	L38	L 7.2.6 Scan for Zombie Processes L 7.2.14 Enforce User Account Control	4,6		
	39	7.3.5 Set Up URL Blocking 7.3.7 Malware Analysis 7.3.9 Signs of Malware Infection 7.3.11 Search Memory Dump for Malware 7.3.13 Create a Virus 7.3.14 Create an HTTP Trojan 7.3.15 Use ProRat to Create a Trojan 7.3.16 Mobile Device Attacks 7.4.1 Beaconing Intrusion	2,4,6		
	L40	L 7.3.3 Counter Malware with Windows Defender L 7.3.4 Configure Windows Defender Application Control L 7.3.6 Configure URL Blocking	4,6		
11	41	7.4.2 Beaconing Intrusion Facts 7.4.3 Create a DNS Tunnel with dnscat2 7.5.1 Social Engineering Overview 7.5.4 Social Engineering Techniques 7.5.7 Phishing and Internet-Based Techniques 7.6.1 Programming and Scripting Overview 7.6.9 Software Development Life Cycle (SDLC) Integration 7.6.11 Assessment and Coding Practices 7.6.13 Reverse Engineering Overview	2,5,6	2	2
	L42	L 7.5.10 Identify Social Engineering	1		
	43	7.6.14 Perform Reverse Engineering	1,4,6		

	7.7.1 Overflow Attacks 7.7.4 Application Attack Mitigation Checklists Facts 8.1.1 Security Information and Event Management (SIEM) Overview 8.1.3 Use Security Onion v2 – Hunter 8.1.4 Use Security Onion v2 – Kibana 8.2.1 Automation Overview 8.2.3 DevSecOps Facts 8.2.5 Automation Technologies			
	L44 L 8.1.5 Evaluate Network Security with Kibana L 8.1.6 Evaluate Network Security with Hunter-1 L 8.1.7 Evaluate Network Security with Hunter-2	1,2,4		
12	45 8.3.1 Abnormal Activity 8.3.3 Endpoint Detection and Response 8.3.9 Suspicious Protocol and Port Usage 8.3.10 Suspicious Protocol and Port Usage Facts 8.3.12 Application-Related Indicators of Compromise 8.3.13 Application-Related Indicators of Compromise Facts 9.1.1 Containment 9.1.3 Eradication 9.1.5 Recovery 9.2.1 Incident Response Training and Testing	1,5	3	1
	L46 L 8.3.11 Analyze FTP Credentials with Wireshark	3		
	47 9.2.3 Incident Response Overview 9.2.4 Incident Response Overview Facts 9.2.6 Incident Response Preparation 9.2.9 Stakeholder Communication Facts 9.2.10 Reporting Requirements Facts 9.2.12 Detection and Analysis 9.3.1 Post-Incident Activities 9.3.7 Digital Forensics Overview	2,5,6		
	48 Review			

* numbers corresponding to Course Learning Outcomes (item 4)